of the foregoing amendments and the following remarks, respectfully requests reconsideration and full allowance of all pending claims.

As a preliminary matter, Applicant notes that Claim 20 has been amended to correct a minor grammatical error, namely, "and" has been added at the end of the second element.

Claims 1-20 stand objected to because of informalities, namely, several extraneous parentheses were present throughout some of the claims, and Claim 7 was dependent upon Claim 8. In response, Applicant has amended Claims 1, 8, 9, 12, 16, and 18 to remove extraneous parenthesis, and Claim 7 has been amended to be dependent upon Claim 1.

Claims 1, 4-10 and 18 stand rejected under 35 U.S.C. § 102(a) as assertedly being anticipated by U.S. Patent No. 5,712,912 to Tomko et al. (hereinafter "Tomko"). Additionally, Claims 2, 3, 11-17, and 19-20 stand rejected under 35 U.S.C. § 103(a) as assertedly being unpatentable over Tomko in view of U.S. Patent No. 54,529,870 to Chaum (hereinafter "Chaum"). In response, Applicant respectfully traverses these rejections.

Rejected independent Claims 1 and 9 have been amended to more particularly recite at least one of the distinguishing characteristics of the present invention, namely, that *an authentication encryptor encrypts a challenge parameter based upon the decrypted security key.* Accordingly, Claims 1 and 9 recite that a biometric measure is made of a current user. The biometric measure is used to decrypt a security key, which was encrypted using a second biometric measure of an authorized user. The decrypted security key is then used to encrypt a challenge parameter. Therefore, the present invention as recited in Claims 1 and 9 encrypts a security key, which can only be correctly decrypted if the biometric measures of the current user are equivalent to the biometric measures of the authorized user, *i.e.*, the current user is an authorized user. The decrypted security key is then used to encrypt the challenge parameter.

Tomko has been cited as fully disclosing Applicant's invention. Tomko, however, *fails to teach or suggest, among other things, a mechanism to encrypt a challenge parameter as claimed in the amended independent Claims 1 and 9.* In contrast to the Applicant's invention, Tomko assertedly decrypts a PIN, which is sent to a device requiring PIN 40. (See Figure 1B.) The processor 204 does not encrypt a challenge parameter as recited in Applicant's independent Claims 1 and 9.

Chaum does not cure the deficiencies of the Tomko disclosure. First, Chaum fails to disclose or suggest an authentication encrypter that encrypts a challenge parameter based upon the decrypted security key. In contrast to Applicant's invention, Chaum assertedly discloses a challenge parameter that is used to generate a key unique to the current identification process. The key is generated from data that may include the challenge parameter, the system key, and/or the random value originally generated in the cryptographic device. (See Chaum, col. 14, lines 34-50.) Chaum, however, fails to disclose or suggest a mechanism(s) that encrypts a security key, decrypts the security key based on a biometric measure, and then encrypts a challenge parameter based on the decrypted security key, as is claimed in Applicant's invention.

Second, even if Chaum did teach or suggest an authentication encrypter that encrypts a challenge parameter based upon the decrypted security key, Chaum is not properly combinable with Tomko. Tomko assertedly discloses a processor 204 (Fig. 2) that provides a decrypted PIN to a device requiring PIN 40. Chaum assertedly discloses a mechanism that accepts a challenge parameter, encrypts the challenge parameter, and provides the encrypted challenge parameter to an external system. In contrast to Applicant's invention as claimed, therefore, *the combination of Chaum and Tomko results in a mechanism that provides a PIN and an encrypted challenge parameter to an external system or a device requiring PIN.*

Applicant's invention, however, decrypts an encrypted security key to yield a decrypted security key. The decrypted security key is utilized to encrypt the challenge parameter, which is then sent to an access device. Therefore, Applicant's invention comprises a mechanism that allows the use of a decrypted security key for encrypting a challenge parameter, providing an additional level of security not present in Chaum and/or Tomko, individually or in combination.

Applicant does not believe any other fees are due; however, in the event that any other fees are due, or that the aforementioned check is absent, insufficient, or unacceptable, the Commissioner is hereby authorized to charge any required fees due (other than issue fees), and to credit any overpayment made, in connection with the filing of this paper to Deposit Account No. 50-0605 of Carr & Storm, L.L.P.

Applicant has now made an earnest attempt to place this application in condition for allowance. For the foregoing reasons and for other reasons clearly apparent, Applicant respectfully requests full allowance of Claims 1, 3-11, and 13-20.

Should the Examiner have any questions or desire clarification of any sort, or deem that any further amendment is desirable to place this application in condition for allowance, the Examiner is invited to telephone the undersigned at the number listed below.

Respectfully submitted,

Dated: 12/20/2001

By: _____

Roger C. Knapp
Reg. No. 46,836
Attorney for Applicants
CARR & STORM, L.L.P.
670 Founders Square
900 Jackson Street
Dallas, Texas 75202
(214) 760-3032 (direct)
(214) 760-3000 (main)
(214) 760-3003 (fax)

Mail PTO Correspondence to:
U.S. Philips Corporation
580 White Plains Road
Tarrytown, N.Y. 10591-5190

AMENDMENT
VERSION WITH MARKINGS TO SHOW CHANGES MADE

1. (AMENDED) A security token comprising:

a biometric sensor that provides a first biometric key of a current user of the security token, based upon a biometric measure of the current user,

a storage element that stores an encryption[()] of a security key, the encryption [()] being based on a second biometric key of an authorized user, [and]

a biometric decrypter, operably coupled to the biometric sensor and the storage element, that decrypts the encryption [()] of the security key, producing thereby a decrypted security key that is equal to the security key when the first biometric key is equivalent to the second biometric key, and

an authentication encrypter, operably coupled to the biometric decrypter, that encrypts a challenge parameter to produce a response parameter that is based upon the decrypted security key.

3. (AMENDED) The security token of claim 1 [2], further including:

a token identifier that provides an identification that is associated with the authorized user.

7. (AMENDED) The security token of claim 1 [8], wherein

the security key is a private key of a set of asymmetric keys that include at least one private key and at least one public key.

8. (AMENDED) The security token of claim 1, further including

a one-time encrypter that produces the encryption [()] of the security key based upon the second biometric key.

9. (AMENDED) A security system comprising:

a token that includes:

a biometric sensor that provides a first biometric key of a current user of the token based upon a biometric measure of the current user,

an encryption [)] of a security key, the encryption [)] being based upon a second biometric key of an authorized user, and

a biometric decrypter that decrypts the encryption [)] of the security key to produce a decrypted security key, such that

the decrypted security key is equivalent to the security key when the first biometric key is equivalent to the second biometric key, [and]

the decrypted security key is an erroneous key when the first biometric key is different from the second biometric key; and

an authentication encrypter, operably coupled to the biometric decrypter, that encrypts a challenge parameter to produce a response parameter that is based upon the decrypted security key; and

an access device that, when operably coupled to the token, determines an access status based upon the decrypted security key.

13. (AMENDED) The security system of claim 11 [12], wherein:

the security key is a first key of a pair of asymmetric keys, and

the receiving device includes:

an authentication decrypter that decrypts the response parameter to produce a decrypted result, the decryption being based upon a second key of the pair of asymmetric keys, and

a comparator that compares the decrypted result with the challenge parameters to determine the access status.

16. (AMENDED) The security system of claim 11, wherein the token further includes:

an encapsulation that obstructs access to components of the token, and

a means for destroying at least one of the second biometric key and the encryption [)] of the security key when the encapsulation is breached.

18. (AMENDED) A method for determining an access status comprising the steps of:

encrypting a security key to produce an encrypted security key [)] based upon a first biometric key of an authorized user into a token,

determining a second biometric key of a current user of the token based upon a biometric measure of the current user,

decrypting the encrypted security key [)] to produce a decrypted security key based upon the second biometric measure, and

determining an access status based upon the decrypted security key.

20. (AMENDED) The method of claim 19, wherein

the security key is a first key of a pair of asymmetric keys,

the step of determining the response parameter includes the step of encrypting the challenge parameter based upon the second biometric key, and

the step of determining the access status includes the steps of:

decrypting the response parameter to produce a decrypted result based upon a second key of the pair of asymmetric keys, and

comparing the decrypted result to the challenge parameter to determine the access status.